# Lattice methods for algebraic modular forms on classical groups

Matthew Greenberg and John Voight

**Abstract** We use Kneser's neighbor method and isometry testing for lattices due to Plesken and Souveigner to compute systems of Hecke eigenvalues associated to definite forms of classical reductive algebraic groups.

## 1 Introduction

Let $Q(x) = Q(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ be an even positive definite integral quadratic form in $n$ variables with discriminant $N$. A subject of extensive classical study, continuing today, concerns the number of representations of an integer by the quadratic form $Q$. To do so, we form the corresponding generating series, called the *theta series* of $Q$:

$$\theta_Q(q) = \sum_{x \in \mathbb{Z}^n} q^{Q(x)} \in \mathbb{Z}[[q]].$$

By letting $q = e^{2\pi i z}$ for $z$ in the upper half-plane $\mathscr{H}$, we obtain a holomorphic function $\theta : \mathscr{H} \to \mathbb{C}$; owing to its symmetric description, this function is a classical modular form of weight $n/2$ and level $4N$. For example, in this way one can study the representations of an integer as the sum of squares via Eisenstein series for small even values of $n$.

Conversely, theta series can be used to understand spaces of classical modular forms. This method goes by the name *Brandt matrices* as it goes back to early work of Brandt and Eichler [17, 18] (the *basis problem*). From the start, Brandt matrices were used to computationally study spaces of modular forms, and explicit

Matthew Greenberg
University of Calgary, 2500 University Drive NW, Calgary, AB, T2N 1N4, Canada, e-mail: mgreenbe@math.ucalgary.ca

John Voight
Department of Mathematics and Statistics, University of Vermont, 16 Colchester Ave, Burlington, VT 05401, USA, e-mail: jvoight@gmail.com

algorithms were exhibited by Pizer [42], Hijikata, Pizer, and Shemanske [25], and Kohel [36]. In this approach, a basis for $S_2(N)$ is obtained by linear combinations of theta series associated to (right) ideals in a quaternion order of discriminant $N$; the Brandt matrices which represent the action of the Hecke operators are obtained via the combinatorial data encoded in the coefficients of theta series. These methods have also been extended to Hilbert modular forms over totally real fields, by Socrates and Whitehouse [49], Dembélé [8], and Dembélé and Donnelly [10].

The connection between such arithmetically-defined counting functions and modular forms is one piece of the Langlands philosophy, which predicts deep connections between automorphic forms in different guises via their Galois representations. In this article, we consider algorithms for computing systems of Hecke eigenvalues in the more general setting of algebraic modular forms, as introduced by Gross [23]. Let $\mathsf{G}$ be a *linear algebraic group* defined over $\mathbb{Q}$, a closed algebraic subgroup of the algebraic group $\mathrm{GL}_n$. (For simplicity now we work over $\mathbb{Q}$, but in the body we work with a group $\mathsf{G}$ defined over a number field $F$; to reduce to this case, one may just take the restriction of scalars.) Let $\mathsf{G}(\mathbb{Z}) = \mathsf{G}(\mathbb{Q}) \cap \mathrm{GL}_n(\mathbb{Z})$ be the group of integral points of $\mathsf{G}$.

Suppose that $\mathsf{G}$ is *connected* as an algebraic variety and *reductive*, so that its maximal connected unipotent normal subgroup is trivial (a technical condition important for the theory). Let $G_\infty = \mathsf{G}(\mathbb{R})$ denote the real points of $\mathsf{G}$. Then $G_\infty$ is a real Lie group with finitely many connected components.

Now we make an important assumption that allows us to compute via arithmetic and lattice methods: we suppose that $G_\infty$ is compact. For example, we may take $\mathsf{G}$ to be a special orthogonal group, those transformations of determinant 1 preserving a positive definite quadratic form over a totally real field, or a unitary group, those preserving a definite Hermitian form relative to a CM extension of number fields. Under this hypothesis, Gross [23] showed that automorphic forms arise without analytic hypotheses and so are called *algebraic modular forms*.

Let $\widehat{\mathbb{Q}} = \mathbb{Q} \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$ be the finite adeles of $\mathbb{Q}$. Let $\widehat{K}$ be a compact open subgroup of $\widehat{G} = \mathsf{G}(\widehat{\mathbb{Q}})$ (a choice of *level*), let $G = \mathsf{G}(\mathbb{Q})$, and let

$$Y = G \backslash \widehat{G} / \widehat{K}.$$

The set $Y$ is finite. Let $W$ be an irreducible (finite-dimensional) representation of $G$. Then the space of *modular forms for* $\mathsf{G}$ *of weight* $W$ *and level* $\widehat{K}$ is

$$M(W, \widehat{K}) = \{ f : \widehat{G}/\widehat{K} \to W \mid f(\gamma g) = \gamma f(g) \text{ for all } \gamma \in G \}.$$

Such a function $f \in M(W, \widehat{K})$ is determined by its values on the finite set $Y$; indeed, if $W$ is the trivial representation, then modular forms are simply functions on $Y$. The space $M(W, \widehat{K})$ is equipped with an action of *Hecke operators* for each double coset $\widehat{K}\widehat{p}\widehat{K}$ with $\widehat{p} \in \widehat{G}$; these operators form a ring under convolution, called the *Hecke algebra*.

Algebraic modular forms in the guise of Brandt matrices and theta series of quaternary quadratic forms, mentioned above, correspond to the case where $G =$

$\mathrm{PGL}_1(B) = B^\times/F^\times$ where $B$ is a definite quaternion algebra over a totally real field $F$. The first more general algorithmic consideration of algebraic modular forms was undertaken by Lanksy and Pollack [37], who computed with the group $\mathsf{G} = \mathrm{PGSp}_4$ and the exceptional group $\mathsf{G} = G_2$ over $\mathbb{Q}$. Cunningham and Dembélé [7] later computed Siegel modular forms over totally real fields using algebraic modular forms, and Loeffler [39] has performed computations with the unitary group $U(2)$ relative to the imaginary quadratic extension $\mathbb{Q}(\sqrt{-11})/\mathbb{Q}$ and $U(3)$ relative to $\mathbb{Q}(\sqrt{-7})/\mathbb{Q}$. In this paper, we consider the case where the group $\mathsf{G}$ arises from a definite special orthogonal or unitary group. Our main idea is the use lattice methods, making these computations efficient. This connection is undoubtedly known to the experts, and our small contribution is make it explicit and discuss the relevant computational aspects. We conjecture that, assuming an appropriate analogue of the Ramanujan-Petersson conjecture, lattice methods will run in polynomial time in the output size. (This is known to be true for Brandt matrices, by work of Kirschmer and the second author [31].)

To illustrate our method as we began, let $Q$ be a positive definite quadratic form in $d$ variables over a totally real field $F$, and let $\mathsf{G} = SO(Q)$ be the special orthogonal group of $Q$ over $F$. (To work instead with unitary groups, we simply work with a Hermitian form instead.) Then $\mathsf{G}$ is a connected reductive group with $G_\infty = \mathsf{G}(F \otimes_{\mathbb{Q}} \mathbb{R})$ compact. Let $\Lambda$ be a $\mathbb{Z}_F$-lattice in $F^d$. Then the stabilizer $\widehat{K} \subset \widehat{G}$ of $\widehat{\Lambda} = \Lambda \otimes_{\mathbb{Z}} \widehat{\mathbb{Q}}$ is an open compact subgroup and the set $Y = G\backslash\widehat{G}/\widehat{K}$ is in natural bijection with the finite set of equivalence classes of lattices in the *genus* of $\Lambda$, the set of lattices which are *locally equivalent* to $\Lambda$.

The enumeration of representatives of the genus of a lattice has been studied in great detail; we use Kneser's neighbor method [34]. (See the beginning of Section 5 for further references to the use of this method.) Let $\mathfrak{p} \subset \mathbb{Z}_F$ be a nonzero prime ideal with residue class field $\mathbb{F}_\mathfrak{p}$. We say that two $\mathbb{Z}_F$-lattices $\Lambda, \Pi \subset F^n$ are $\mathfrak{p}$-*neighbors* if we have $\mathfrak{p}\Lambda, \mathfrak{p}\Pi \subset \Lambda \cap \Pi$ and

$$\dim_{\mathbb{F}_\mathfrak{p}} \Lambda/(\Lambda \cap \Pi) = \dim_{\mathbb{F}_\mathfrak{p}} \Pi/(\Lambda \cap \Pi) = 1.$$

The $\mathfrak{p}$-neighbors of $\Lambda$ are easy to construct, are locally equivalent to $\Lambda$, and by strong approximation, every class in the genus is represented by a $\mathfrak{p}$-neighbor for some $\mathfrak{p}$. In fact, by the theory of elementary divisors, the Hecke operators are also obtained as a summation over $\mathfrak{p}$-neighbors. Therefore the algorithmic theory of lattices is armed and ready for application to computing automorphic forms.

The main workhorse in using $\mathfrak{p}$-neighbors in this way is an algorithm for isometry testing between lattices (orthogonal, Hermitian, or otherwise preserving a quadratic form). For this, we rely on the algorithm of Plesken and Souvignier [43], which matches up short vectors and uses other tricks to rule out isometry as early as possible. This algorithm was implemented in Magma [2] by Souvignier, with further refinements to the code contributed by Steel, Nebe, and others.

These methods also apply to compact forms of symplectic groups; see Chisholm [3]. We anticipate that these methods can be generalized to a wider class of reductive

groups, and believe that such an investigation would prove valuable for explicit investigations in the Langlands program.

The outline of this paper is as follows. In Section 2, we give basic terminology and notation for algebraic modular forms. In section 3, we review orthogonal and unitary groups and their Hecke theory. In section 4 we discuss elementary divisors in preparation for section 5, where we give an exposition of Kneser's neighbor method and translate Hecke theory to the lattice setting. In section 6, we present the algorithm, and we conclude in section 7 with some explicit examples.

## 2 Algebraic modular forms

In this first section, we define algebraic modular forms; a reference is the original work of Gross [23].

### *Algebraic modular forms*

Let $F$ be a totally real number field and let

$$F_\infty = F \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{[F:\mathbb{Q}]}.$$

Let $\widehat{\mathbb{Q}} = \mathbb{Q} \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$ be the finite adeles of $\mathbb{Q}$, let $\widehat{F} = F \otimes_{\mathbb{Q}} \widehat{\mathbb{Q}}$ be the ring of finite adeles of $F$.

Let $\mathsf{G}$ be a connected, reductive algebraic group over $F$. We make the important and nontrivial assumption that the Lie group $G_\infty = G(F_\infty)$ is compact. Let $\widehat{G} = \mathsf{G}(\widehat{F})$ and $G = \mathsf{G}(F)$.

Let $\rho : G \to W$ be an irreducible (finite-dimensional) representation of $G$ defined over a number field $E$.

**Definition 2.1.** The space of *algebraic modular forms for $G$ of weight $W$* is

$$M(\mathsf{G}, W) = \left\{ f : \widehat{G} \to W \;\middle|\; \begin{array}{l} f \text{ is locally constant and} \\ f(\gamma\widehat{g}) = \gamma f(\widehat{g}) \text{ for all } \gamma \in G \text{ and } \widehat{g} \in \widehat{G} \end{array} \right\}.$$

We will often abbreviate $M(W) = M(\mathsf{G}, W)$.

Each $f \in M(W)$ is constant on the cosets of a compact open subgroup $\widehat{K} \subset \widehat{G}$, so $M(W)$ is the direct limit of the spaces

$$M(W, \widehat{K}) = \left\{ f : \widehat{G} \to W \;\middle|\; \begin{array}{c} f(\gamma\widehat{g}\widehat{u}) = \gamma f(\widehat{g}) \\ \text{for all } \gamma \in G,\ \widehat{g} \in \widehat{G},\ \widehat{u} \in \widehat{K} \end{array} \right\}. \tag{1}$$

of modular forms of *level* $\widehat{K}$. We will consider these smaller spaces, so let $\widehat{K} \subset \widehat{G}$ be an open compact subgroup. When $W = E$ is the trivial representation, $M(W,\widehat{K})$ is simply the space of $E$-valued functions on the space $Y = G\backslash\widehat{G}/\widehat{K}$.

**Proposition 2.2 ([23, Proposition 4.3]).** *The set $Y = G\backslash\widehat{G}/\widehat{K}$ is finite.*

Let $h = \#Y$. Writing

$$\widehat{G} = \bigsqcup_{i=1}^{h} G\widehat{x}_i\widehat{K}, \tag{2}$$

it follows from the definition that any $f \in M(W,\widehat{K})$ is completely determined by the elements $f(\widehat{x}_i)$ with $i = 1,\ldots,h$. Let

$$\Gamma_i = G \cap \widehat{x}_i\widehat{K}\widehat{x}_i^{-1}.$$

The (arithmetic) group $\Gamma_i$, as a discrete subgroup of the compact group $G_\infty$, is finite [23, Proposition 1.4].

**Lemma 2.3.** *The map*

$$\begin{aligned} M(W,\widehat{K}) &\longrightarrow \bigoplus_{i=1}^{h} H^0(\Gamma_i,W) \\ f &\mapsto (f(\widehat{x}_1),\ldots,f(\widehat{x}_h)) \end{aligned}$$

*is an isomorphism of $F$-vector spaces, where*

$$H^0(\Gamma_i,W) = \{v \in W : \gamma v = v \text{ for all } \gamma \in \Gamma_i\}.$$

In particular, from Lemma 2.3 we see that $M(W,\widehat{K})$ is finite-dimensional as an $E$-vector space.

## *Hecke operators*

The space $M(W,\widehat{K})$ comes equipped with the action of Hecke operators, defined as follows. Let $\mathscr{H}(\widehat{G},\widehat{K}) = \mathscr{H}(\widehat{K})$ be the space of locally constant, compactly supported, $\widehat{K}$-bi-invariant functions on $\widehat{G}$. Then $\mathscr{H}(\widehat{G},\widehat{K})$ is a ring under convolution, called the *Hecke algebra*, and is generated by the characteristic functions $T(\widehat{p})$ of double cosets $\widehat{K}\widehat{p}\widehat{K}$ for $\widehat{p} \in \widehat{G}$. Given such a characteristic function $T(\widehat{p})$, decompose the double coset $\widehat{K}\widehat{p}\widehat{K}$ into a disjoint union of right cosets

$$\widehat{K}\widehat{p}\widehat{K} = \bigsqcup_{j} \widehat{p}_j\widehat{K} \tag{3}$$

and define the action of $T(\widehat{p})$ on $f \in M(W,\widehat{K})$ by

$$(T(\widehat{p})f)(\widehat{g}) = \sum_j f(\widehat{g}\widehat{p}_j). \tag{4}$$

This action is well-defined (independent of the choice of representative $\widehat{p}$ and representatives $\widehat{p}_j$) by the right $\widehat{K}$-invariance of $f$. Finally, a straightforward calculation shows that the map in Lemma 2.3 is Hecke equivariant.

## *Level*

There is a natural map which relates modular forms of higher level to those of lower level by modifying the coefficient module, as follows [12, §8]. Suppose that $\widehat{K}' \leq \widehat{K}$ is a finite index subgroup. Decomposing as in (2), we obtain a bijection

$$\begin{aligned} G\backslash\widehat{G}/\widehat{K}' = \bigsqcup_{i=1}^{h} G\backslash\left(G\widehat{x}_i\widehat{K}\right)/\widehat{K}' &\xrightarrow{\sim} \bigsqcup_{i=1}^{h} \Gamma_i\backslash\widehat{K}_i/\widehat{K}_i' \\ G(\gamma\widehat{x}_i\widehat{u})\widehat{K}' &\mapsto \Gamma_i(\widehat{x}_i\widehat{u}\widehat{x}_i^{-1})\widehat{K}_i' \end{aligned}$$

for $\gamma \in G$ and $\widehat{u} \in \widehat{K}$. This yields

$$M(W,\widehat{K}') \xrightarrow{\sim} H^0(\Gamma_i, \mathrm{Hom}(\widehat{K}_i/\widehat{K}_i', W)) \cong \bigoplus_{i=1}^{h} H^0(\Gamma_i, \mathrm{Coind}_{\widehat{K}_i'}^{\widehat{K}_i} W).$$

Via the obvious bijection

$$\widehat{K}_i/\widehat{K}_i' \cong \widehat{K}/\widehat{K}', \tag{5}$$

letting $W = \mathrm{Coind}_{\widehat{K}'}^{\widehat{K}} W$ we can also write

$$M(W,\widehat{K}') \cong \bigoplus_{i=1}^{h} H^0(\Gamma_i, W_i) \tag{6}$$

where $W_i$ is the representation $W$ with action twisted by the identification (5). Moreover, writing $\widehat{K} = (K_{\mathfrak{p}})_{\mathfrak{p}}$ in terms of its local components, for any Hecke operator $T(\widehat{p})$ such that

$$\text{if } \widehat{p} \notin K_{\mathfrak{p}}' \text{ then } K_{\mathfrak{p}} = K_{\mathfrak{p}}'$$

(noting that $\widehat{p} \in K_{\mathfrak{p}}'$ for all but finitely many primes $\mathfrak{p}$), the same definition (4) applies and by our hypothesis we have a simultaneous double coset decomposition

$$\widehat{K}'\widehat{p}\widehat{K}' = \bigsqcup_j \widehat{p}_j\widehat{K}' \quad \text{and} \quad \widehat{K}\widehat{p}\widehat{K} = \bigsqcup_j \widehat{p}_j\widehat{K}.$$

Now, comparing (6) to the result of Lemma 2.3, we see in both cases that modular forms admit a uniform description as $h$-tuples of $\Gamma_i$-invariant maps. For this reason, a special role in our treatment will be played by maximal open compact subgroups.

## *Automorphic representations*

As it forms one of the core motivations of our work, we conclude this section by briefly describing the relationship between the spaces $M(W)$ of modular forms and automorphic representations of $\mathsf{G}$. Suppose that $W$ is defined over $F$ (cf. Gross [23, §3]). Since $G_\infty$ is compact, by averaging there exists a symmetric, positive-definite, $G_\infty$-invariant bilinear form

$$\langle , \rangle : W_\infty \times W_\infty \longrightarrow F_\infty.$$

where $W_\infty = W \otimes_F F_\infty$. Then we have a linear map

$$\Psi : M(W) \longrightarrow \mathrm{Hom}_{G_\infty}(W_\infty, L^2(G\backslash(\widehat{G} \times G_\infty), F_\infty))$$

by

$$\Psi(f)(v)(\widehat{g}, g_\infty) = \langle \rho(g_\infty)v, f(\widehat{g}) \rangle$$

for $f \in M(W)$, $v \in W$, and $(\widehat{g}, g_\infty) \in \widehat{G} \times G_\infty$. The Hecke algebra $\mathscr{H}(\widehat{K})$ acts on the representation space

$$\mathrm{Hom}_{G_\infty}(W_\infty, L^2(G\backslash(\widehat{G} \times G_\infty), F_\infty))$$

via its standard action on $L^2$ by convolution.

Now, for a nonzero $v \in W_\infty$, define

$$\begin{aligned} \Psi_v : M(W) &\to L^2(G\backslash(\widehat{G} \times G_\infty), F_\infty) \\ f &\mapsto \Psi(f)(v). \end{aligned}$$

(In practice, it is often convenient to take $v$ to be a highest weight vector.)

**Proposition 2.4.** *The map $\Psi_v$ is $\mathscr{H}(\widehat{K})$-equivariant and induces a bijection between irreducible $\mathscr{H}(\widehat{K})$-submodules of $M(W, \widehat{K})$ and automorphic representations $\pi$ of $\mathsf{G}(\mathbf{A}_F)$ such that*

(i) *$\pi(\widehat{K})$ has a nonzero fixed vector, and*
(ii) *$\pi_\infty$ is isomorphic to $\rho_\infty$.*

In particular, an $\mathscr{H}(\widehat{K})$ eigenvector $f \in M(W, \widehat{K})$ gives rise to an automorphic representation. Since automorphic representations are of such fundamental importance, explicit methods to decompose $M(W, \widehat{K})$ into its Hecke eigenspaces are of significant interest.

## 3 Hermitian forms, classical groups, and lattices

Having set up the general theory in the previous section, we now specialize to the case of orthogonal and unitary groups. In this section, we introduce these classical groups; basic references are Borel [1] and Humphreys [26].

### *Classical groups*

Let $F$ be a field with $\mathrm{char} F \neq 2$ and let $L$ be a commutative étale $F$-algebra equipped with an involution $\bar{\ }: L \to L$ such that $F$ is the fixed field of $L$ under $\bar{\ }$. Then there are exactly three possibilities for $L$:

1. $L = F$ and $\bar{\ }$ is the identity;
2. $L$ is a quadratic field extension of $F$ and $\bar{\ }$ is the nontrivial element of $\mathrm{Gal}(L/F)$; or
2′. $L \cong F \times F$ and $\overline{(b,a)} = (a,b)$ for all $(a,b) \in F \times F$.

(As étale algebras, cases 2 and 2′ look the same, but we will have recourse to single out the split case.)

Let $V$ be a finite-dimensional vector space over $L$. Let

$$\varphi : V \times V \longrightarrow L$$

be a *Hermitian form* relative to $L/F$, so that:

(i) $\varphi(x+y,z) = \varphi(x,z) + \varphi(y,z)$ for all $x,y,z \in V$;
(ii) $\varphi(ax,y) = a\varphi(x,y)$ for all $x,y \in V$ and $a \in L$; and
(iii) $\varphi(y,x) = \overline{\varphi(x,y)}$ for all $x,y \in V$.

Further suppose that $\varphi$ is *nondegenerate*, so $\varphi(x,V) = \{0\}$ for $x \in V$ implies $x = 0$. For example, the *standard* nondegenerate Hermitian form on $V = L^n$ is

$$\varphi(x,y) = \sum_{i=1}^{n} x_i \overline{y_i}. \tag{7}$$

Let $\mathsf{A}$ be the (linear) algebraic group of automorphisms of $(V,\varphi)$ over $F$: that is to say, for a commutative $F$-algebra $D$, we have

$$\mathsf{A}(D) = \mathrm{Aut}_{D\otimes_F L}(V_F \otimes_F D, \varphi).$$

(Note the tensor product is over $F$, so in particular we consider $V$ as an $F$-vector space and write $V_F$.) More explicitly, we have

$$\mathsf{A}(F) = \mathrm{Aut}_L(V,\varphi) = \{T \in \mathrm{GL}(V) : \varphi(Tx,Ty) = \varphi(x,y)\}.$$

Since $\varphi$ is nondegenerate, for every linear map $T : V \to V$, there is a unique linear map $T^* : V \to V$ such that

$$\varphi(Tx, y) = \varphi(x, T^* y)$$

for all $x, y \in V$. It follows that

$$\mathsf{A}(F) = \{T \in \mathrm{GL}(V) : TT^* = 1\}$$

where the $^*$ depends on $\varphi$.

The group $\mathsf{A}$ is reductive but is not connected in case 1. Let $\mathsf{G}$ be the connected component of the identity in $\mathsf{A}$.

In each of the three cases, we have the following description of $\mathsf{G} \leq \mathsf{A}$.

1. If $L = F$, then $\varphi$ is a symmetric bilinear form over $F$ and $\mathsf{G} = \mathsf{SO}(\varphi) \leq \mathsf{O}(\varphi) = \mathsf{A}$ are the special orthogonal and orthogonal group of the form $\varphi$.
2. If $L$ is a quadratic field extension of $F$, then $\varphi$ is a Hermitian form with respect to $L/F$ and $\mathsf{G} = \mathsf{U}(\varphi) = \mathsf{A}$ is the unitary group associated to $\varphi$.

2′. If $L = F \times F$, then actually we obtain a general linear group. Indeed, let $e_1 = (1,0)$ and $e_2 = (0,1)$ be an $F$-basis of idempotents of $L$. Then $V_1 = e_1 V$ and $V_2 = e_2 V$ are vector spaces over $F$, and the map $T \mapsto T|_{V_1}$ gives an isomorphism of $\mathsf{G} = \mathsf{A}$ onto $\mathsf{GL}(V_1)$.

*Remark 3.1.* It would also be profitable to consider other groups of symmetries of $(V, \varphi)$, for example, the spin group $\mathsf{Spin}(\varphi)$ in case 1 and the special unitary group $\mathsf{SU}(\varphi)$ in case 2. We have simply made one such choice for the purposes of this article.

*Remark 3.2.* To obtain symplectic or skew-Hermitian forms, we would work instead with signed Hermitian forms above.

*Remark 3.3.* We have phrased the above in terms of Hermitian forms, but one could instead work with their associated quadratic forms $Q : V \to L$ defined by $Q(v) = \varphi(v, v)$. In characteristic 2, working with quadratic forms has some advantages, but in any case we will be working in situations where the two perspectives are equivalent.

## *Integral structure*

Suppose now that $F$ is a number field with ring of integers $\mathbb{Z}_F$. By a *prime* of $F$ we mean a nonzero prime ideal of $\mathbb{Z}_F$.

Let $(V, \varphi)$ and $\mathsf{G} \leq \mathsf{A}$ be as above. Since our goal is the calculation of algebraic modular forms, we insist that $G_\infty = \mathsf{G}(F_\infty) = \mathsf{G}(F \otimes_{\mathbb{Q}} \mathbb{R})$ be compact, which rules out the case 2′ (that $L = F \times F$) and requires that $F$ be totally real.

Let $\mathbb{Z}_L$ be the ring of integers of $L$. Let $\Lambda \subset V$ be a *lattice* in $V$, a projective $\mathbb{Z}_L$-module with rank equal to the dimension of $V$. Suppose further that $\Lambda$ is *integral*, so $\varphi(\Lambda,\Lambda) \subseteq \mathbb{Z}_L$. Define the *dual lattice* by

$$\Lambda^\# = \{x \in V : \varphi(\Lambda, x) \subseteq \mathbb{Z}_L\}.$$

We say $\Lambda$ is *unimodular* if $\Lambda^\# = \Lambda$.

To a lattice $\Pi \subseteq V$ we associate the the lattice

$$\widehat{\Pi} = \Pi \otimes_{\mathbb{Z}_L} \widehat{\mathbb{Z}}_L \subset \widehat{V} = V \otimes_L \widehat{L}$$

with $\Pi_\mathfrak{p} = \Pi \otimes_{Z_L} \mathbb{Z}_{L,\mathfrak{p}}$; we have $\Pi \otimes_{\mathbb{Z}_L} \mathbb{Z}_{L,\mathfrak{p}} = \Lambda \otimes_{\mathbb{Z}_L} \mathbb{Z}_{L,\mathfrak{p}}$ for all but finitely primes $\mathfrak{p}$. Conversely, given a lattice $(\Pi_\mathfrak{p})_\mathfrak{p} \subseteq \widehat{V}$ with $\Pi_\mathfrak{p} = \Lambda \otimes_{\mathbb{Z}_L} \mathbb{Z}_{L,\mathfrak{p}}$ for all but finitely many $\mathfrak{p}$, we obtain a lattice

$$\Pi = \{x \in V : x \in \Pi_\mathfrak{p} \text{ for all } \mathfrak{p}\}.$$

(In fact, one can take this intersection over all localizations in $V$, not completions, but we do not want to confuse notation.) These associations are mutually inverse to one another (*weak approximation*), so we write $\widehat{\Pi} = (\Pi_\mathfrak{p})_\mathfrak{p}$ unambiguously.

Let

$$\widehat{K} = \{\widehat{g} \in \widehat{G} : \widehat{g}\widehat{\Lambda} = \widehat{\Lambda}\} \tag{8}$$

be the stabilizer of $\widehat{\Lambda}$ in $\widehat{G}$. Then $\widehat{K}$ is an open compact subgroup of $\widehat{G}$. Further, let

$$\Gamma = \{g \in G : g\Lambda = \Lambda\}$$

be the stabilizer of $\Lambda$ in $G$. Then the group $\Gamma$ is finite, since it is a discrete subgroup of the compact group $G_\infty$ [23, Proposition 1.4].

*Remark 3.4.* In fact, by work of Gan and Yu [21, Proposition 3.7], there is a unique smooth linear algebraic group $\underline{\mathsf{A}}$ over $\mathbb{Z}_F$ with generic fiber $\mathsf{A}$ such that for any commutative $\mathbb{Z}_F$-algebra $D$ we have

$$\underline{\mathsf{A}}(D) = \mathrm{Aut}_{D \otimes_{\mathbb{Z}_F} \mathbb{Z}_L}(\Lambda \otimes_{\mathbb{Z}_L} D, \varphi).$$

As we will not make use of this, we do not pursue integral models of $\mathsf{A}$ any further here.

We now consider the extent to which a lattice is determined by all of its localizations in this way: this extent is measured by the genus, which is in turn is given by a double coset as in Section 2, as follows.

**Definition 3.5.** Let $\Lambda$ and $\Pi$ be lattices in $V$. We say $\Lambda$ and $\Pi$ are ($G$-)*equivalent* (or *isometric*) if there exists $\gamma \in G$ such that $\gamma\Lambda = \Pi$. We say $\Lambda$ and $\Pi$ are *locally equivalent* (or *locally isometric*) if there exists $\widehat{g} \in \widehat{G}$ such that $\widehat{g}\widehat{\Lambda} = \widehat{\Pi}$. The set of all lattices locally equivalent to $\Lambda$ is called the *genus* of $\Lambda$ and is denoted $\mathrm{gen}(\Lambda)$.

For any $\widehat{g} = (g_\mathfrak{p})_\mathfrak{p} \in \widehat{G}$, we have

$$\widehat{g}\widehat{\Lambda} = \prod_\mathfrak{p} g_\mathfrak{p}\Lambda_\mathfrak{p};$$

since $g_\mathfrak{p}\Lambda_\mathfrak{p} = \Lambda_\mathfrak{p}$ for all but finitely many $\mathfrak{p}$, by weak approximation, there is a unique lattice $\Pi \subseteq V$ such that $\widehat{\Pi} = \widehat{g}\widehat{\Lambda}$. By definition, $\Pi \in \mathrm{gen}(\Lambda)$ and every lattice $\Pi \in \mathrm{gen}(\Lambda)$ arises in this way. Thus, the rule

$$(\widehat{g}, \Lambda) \mapsto \Pi = \widehat{g}\Lambda$$

gives an action of $\widehat{G}$ on $\mathrm{gen}(\Lambda)$. The stabilizer of $\Lambda$ under this action is by definition $\widehat{K}$, therefore the mapping

$$\begin{aligned} \widehat{G}/\widehat{K} &\to \mathrm{gen}(\Lambda) \\ \widehat{g}\widehat{K} &\mapsto \widehat{g}\Lambda \end{aligned}$$

is a bijection of $G$-sets. The set $G\backslash\mathrm{gen}(\Lambda)$ of isometry classes of lattices in $\mathrm{gen}(\Lambda)$ is therefore in bijection with the double-coset space (*class set*)

$$Y = G\backslash\widehat{G}/\widehat{K}.$$

By Proposition 2.2 (or a direct argument, e.g. Iyanaga [27, 6.4] for the Hermitian case), the genus $\mathrm{gen}(\Lambda)$ is the union of finitely many equivalence classes called the *class number* of $\Lambda$, denoted $h = h(\Lambda)$.

In this way, we have shown that an algebraic modular form $f \in M(W, \widehat{K})$ can be viewed as a function on $\mathrm{gen}(\Lambda)$. Translating the results of Section 1 in this context, if $\Lambda_1, \ldots, \Lambda_h$ are representatives for the equivalence classes in $\mathrm{gen}(\Lambda)$, then a map $f : \mathrm{gen}(\Lambda) \to W$ is determined by the finite set $f(\Lambda_1), \ldots, f(\Lambda_h)$ of elements of $W$. The problem of enumerating this system of representatives for $Y$ becomes the problem of enumerating representatives for the equivalence classes in $\mathrm{gen}(\Lambda)$, a problem which we will turn to in Section 5 after some preliminary discussion of elementary divisors in Section 4.

## 4 Elementary divisors

In this section, we give the basic setup between elementary divisors and Hecke operators, providing a link to the neighbor method in the lattice setting. The results are standard. We work in the local case.

Let $F$ be a local field of mixed characteristic with ring of integers $\mathbb{Z}_F$, let $\varphi$ be a Hermitian form on $V$ relative to $L/F$, and let $\mathbb{Z}_L$ be the integral closure of $\mathbb{Z}_F$ in $L$ with uniformizer $P$.

Suppose that $G$ is split, and let $T_s \subset G$ be a maximal split torus in $G$. Let $W_s$ be the Weyl group of $(G_s, T_s)$. Let

$$X_*(T_s) = \mathrm{Hom}(T_s, \mathbb{G}_m) \quad \text{and} \quad X^*(T_s) = \mathrm{Hom}(\mathbb{G}_m, T_s)$$

be the groups of characters and cocharacters of $T_s$, respectively.

**Theorem 4.1.** *The Cartan decomposition holds:*

$$G = \bigsqcup_{\lambda \in X^*(T_s)/W_s} K\lambda(P)K.$$

There is a standard method for producing a fundamental domain for the acton of $W_s$ on $X_*(T_s)$, allowing for a more explicit statement of the Cartan decomposition. Let $\Phi^+ \subseteq X^*(T_s)$ be a set of positive roots and let

$$Y_s^+ = \{\lambda \in X_*(T_s) : \lambda(\alpha) \geq 0 \text{ for all } \alpha \in \Phi^+\}.$$

**Proposition 4.2.** *$Y^+$ is a fundamental domain for the action of $W_s$ on $X_*(T_s)$. Therefore, we have*

$$G = \bigsqcup_{\lambda \in Y^+} K\lambda(P)K.$$

We now proceed to analyze this decomposition in Proposition 4.2 explicitly in our situation. We suppose that $\Lambda$ is unimodular (in our methods, we will consider the completions at primes not dividing the discriminant), and we consider two cases.

We first consider the split case ($2'$) with $L \cong F \times F$. Let

$$V_1 = e_1 V \cong F^n \quad \text{and} \quad \Lambda_1 = e_1 \Lambda \cong \mathbb{Z}_F^n.$$

Recall that $T \mapsto T|_{V_1}$ identifies $G = \mathsf{G}(F)$ with $\mathrm{GL}(V_1)$. Already having described $V_1$ and $\Lambda_1$ in terms of coordinates we have

$$G = \mathrm{GL}_d(F) \quad \text{and} \quad K = \mathrm{GL}_d(\mathbb{Z}_F).$$

Let $T \leq G$ be the subgroup of diagonal matrices, consisting of elements $t = \mathrm{diag}(t_1, \ldots, t_n)$. For $i = 1, \ldots, n$, define the cocharacter $\lambda_i : F^\times \to T$ by

$$\lambda_i(a) = \mathrm{diag}(1, \ldots, 1, a, 1, \ldots, 1),$$

where $a$ occurs in the $i$-th component. Then

$$Y_s^+ = \{\lambda_1^{r_1} \cdots \lambda_n^{r_n} : r_1 \leq \cdots \leq r_n\}.$$

**Proposition 4.3 (Elementary divisors; split case).** *Let $\Lambda$ and $\Pi$ be unimodular lattices in $V$ with $L \cong F \times F$. Then there is a basis*

$$e_1, \ldots, e_n$$

*of $\Lambda$ and integers*

$$r_1 \leq \cdots \leq r_n$$

*such that*

$$(\overline{P}/P)^{r_1}e_1,\dots,(\overline{P}/P)^{r_n}e_n$$

*is a basis of $\Pi$. Moreover, the sequence $r_1 \le \cdots \le r_n$ is uniquely determined by $\Lambda$ and $\Pi$.*

Now we consider the more difficult cases (1) and (2), which we can consider uniformly. We have that either $L = F$ or the maximal ideal of $\mathbb{Z}_F$ is inert or ramified in $\mathbb{Z}_L$. Let $\nu = \nu(\varphi)$ be the *Witt index* of $(V,\varphi)$, the dimension of a maximal isotropic subspace. Then $\nu = \dim T_s \le n/2$ and $V$ admits a basis of the form

$$e_1,\dots,e_\nu,g_1,\dots,g_{n-2\nu},f_1,\dots,f_\nu$$

such that

$$\varphi(e_i,e_j) = \varphi(f_i,f_j) = 0 \quad \text{and} \quad \varphi(e_i,f_j) = \delta_{ij}.$$

In this basis, the matrix $\varphi$ is

$$A(\varphi) = \begin{pmatrix} & & I \\ & \big(\varphi(g_i,g_j)\big)_{i,j} & \\ I & & \end{pmatrix}$$

where $I$ is the $\nu \times \nu$ identity matrix. The set of matrices of the form

$$\begin{pmatrix} \operatorname{diag}(t_1,\dots,t_\nu) & & \\ & I & \\ & & \operatorname{diag}(\overline{t}_1,\dots,\overline{t}_\nu)^{-1} \end{pmatrix}$$

constitute a maximal split torus in $G$. Considering $\lambda_i$ as a cocharacter of $\mathrm{GL}_\nu(F)$ as above, define

$$\begin{aligned} \mu_i : F^\times &\to T \\ a &\mapsto \mu_i(a) = \begin{pmatrix} \lambda_i(a) & & \\ & I & \\ & & \lambda_i(\overline{a})^{-1} \end{pmatrix}. \end{aligned}$$

With these choices, we have

$$Y_s^+ = \{\mu_1^{r_1}\cdots\mu_\nu^{r_n} : r_1 \le \cdots \le r_\nu\}.$$

**Proposition 4.4 (Elementary divisors; nonsplit case).** *Let $\Lambda$ and $\Pi$ be unimodular lattices in $V$ with $L \ncong F \times F$. Then there is a basis*

$$e_1,\dots,e_\nu,g_1,\dots,g_{n-2\nu},f_1,\dots,f_\nu$$

*of $\Lambda$ and integers*

$$r_1 \le \cdots \le r_\nu$$

*such that*

$$\overline{P}^{r_1}e_1,\dots,\overline{P}^{r_v}e_v,g_1,\dots,g_j,P^{-r_1}f_1,\dots,P^{-r_v}f_v$$

*is a basis of $\Pi$. Moreover, the sequence $r_1 \le \cdots \le r_v$ is uniquely determined by $\Lambda$ and $\Pi$.*

## 5 Neighbors, lattice enumeration, and Hecke operators

In this section, we describe the enumeration of representatives for equivalence classes in the genus of a Hermitian lattice. We develop the theory of neighbors with an eye to computing Hecke operators in the next section.

The original idea of neighbors is due to Kneser [34], who wished to enumerate the genus of a (positive definite) quadratic form over $\mathbb{Z}$. Schulze-Pillot [47] implemented Kneser's method as an algorithm to compute the genus of ternary and quaternary quadratic forms over $\mathbb{Z}$, and Scharlau and Hemkemeier [46] developed effective methods to push this into higher rank. For Hermitian forms, Iyanaga [28] used Kneser's method to compute the class numbers of unimodular positive definite Hermitian forms over $\mathbb{Z}[i]$ of dimensions $\le 7$; later Hoffmann [24] pursued the method more systematically with results for imaginary quadratic fields of discriminants $d = -3$ to $d = -20$ and Schiemann [45] extended these computations further for imaginary quadratic fields (as far as $d = -455$). For further reference on lattices, see also O'Meara [41, Chapter VIII], Knus [32], Shimura [48], and Scharlau [44].

### *Neighbors and invariant factors*

Let $F$ be a number field with ring of integers $\mathbb{Z}_F$. Let $\mathbb{Z}_L$ be a field containing $F$ with $[L:F] \le 2$, ring of integers $\mathbb{Z}_L$, and involution $\bar{}$ with fixed field $F$. In particular, we allow the case $L = F$ and $\mathbb{Z}_L = \mathbb{Z}_F$. Let $\varphi$ be a Hermitian form on $V$ relative to $L/F$, and let $\Lambda \subset V$ be an integral lattice.

If $\Pi \subset V$ is another lattice, then there exists a basis $e_1,\dots,e_n$ for $V$ and fractional ideals $\mathfrak{A}_1,\dots,\mathfrak{A}_n$ and $\mathfrak{B}_1,\dots,\mathfrak{B}_n$ of $\mathbb{Z}_L$ such that

$$\Lambda = \mathfrak{A}_1 e_1 \oplus \cdots \oplus \mathfrak{A}_n e_n$$

and

$$\Pi = \mathfrak{B}_1 e_1 \oplus \cdots \oplus \mathfrak{B}_n e_n$$

(a direct sum, not necessarily an orthogonally direct sum) satisfying

$$\mathfrak{B}_1/\mathfrak{A}_1 \supseteq \cdots \supseteq \mathfrak{B}_n/\mathfrak{A}_n.$$

The sequence $\mathfrak{B}_1/\mathfrak{A}_1,\dots,\mathfrak{B}_n/\mathfrak{A}_n$ is uniquely determined and called the *invariant factors* of $\Pi$ relative to $\Lambda$. Note that $\Pi \subseteq \Lambda$ if and only if the invariant factors are integral ideals of $\mathbb{Z}_L$.

Define the fractional ideal

$$\mathfrak{d}(\Lambda,\Pi)=\prod_{i=1}^{n}\mathfrak{B}_i/\mathfrak{A}_i$$

and let $\mathfrak{d}(\Lambda)=\mathfrak{d}(\Lambda^{\#},\Lambda)$, where $\Lambda^{\#}\supseteq\Lambda$ is the dual lattice of $\Lambda$. Then in fact $\overline{\mathfrak{d}(\Lambda)}=\mathfrak{d}(\Lambda)$, so $\mathfrak{d}(\Lambda)$ arises from an ideal over $\mathbb{Z}_F$, which we also denote $\mathfrak{d}(\Lambda)$ and call the *discriminant* of $\Lambda$. In particular, $\Lambda$ is unimodular if and only if $\mathfrak{d}(\Lambda)=\mathbb{Z}_F$, and more generaly $\Lambda_{\mathfrak{p}}=\Lambda\otimes_{\mathbb{Z}_F}\mathbb{Z}_{F,\mathfrak{p}}$ is unimodular whenever $\mathfrak{p}$ is a prime of $F$ with $\mathfrak{p}\nmid\mathfrak{d}(\Lambda)$.

**Definition 5.1.** Let $\mathfrak{P}$ be a prime of $L$ and let $k\in\mathbb{Z}$ with $0\le k\le n$. An integral lattice $\Pi\subset V$ is a $\mathfrak{P}^k$-neighbor of $\Lambda$ if $\Pi$ has $k$ invariant factors $\overline{\mathfrak{P}}$ and $\mathfrak{P}^{-1}$, i.e., invariant factors

$$\underbrace{\overline{\mathfrak{P}},\dots,\overline{\mathfrak{P}}}_{k},S,\dots,S,\underbrace{\mathfrak{P}^{-1},\dots,\mathfrak{P}^{-1}}_{k}$$

if $k\le n/2$ and

$$\underbrace{\overline{\mathfrak{P}},\dots,\overline{\mathfrak{P}}}_{n-k},\underbrace{\overline{\mathfrak{P}}\mathfrak{P}^{-1},\dots,\overline{\mathfrak{P}}\mathfrak{P}^{-1}}_{2k-n},\underbrace{\mathfrak{P}^{-1},\dots,\mathfrak{P}^{-1}}_{n-k}$$

if $k>n/2$ and $\mathfrak{P}\neq\overline{\mathfrak{P}}$.

We require that $\mathfrak{P}\neq\overline{\mathfrak{P}}$ if $k>n/2$ because the maximal isotropic subspaces in this case have dimension $\le n/2$, by Proposition 4.4. It follows from a comparison of invariant factors that $\Pi$ is a $\mathfrak{P}^k$-neighbor of $\Lambda$ if and only if

$$\Pi/(\Lambda\cap\Pi)\cong(\mathbb{Z}_L/\mathfrak{P})^k \text{ and } \Lambda/(\Lambda\cap\Pi)\cong(\mathbb{Z}_L/\overline{\mathfrak{P}})^k.$$

A $\mathfrak{P}$-neighbor $\Pi$ of $\Lambda$ has the same discriminant $\mathfrak{d}(\Lambda)=\mathfrak{d}(\Pi)$.

*Remark 5.2.* One may also define $N$-neighbors for $N$ a finitely generated torsion $\mathbb{Z}_L$-module.

## *Neighbors and isotropic subspaces*

Let $\mathfrak{P}$ be prime of $L$ above $\mathfrak{p}$ and let $\mathfrak{q}=\mathfrak{P}\overline{\mathfrak{P}}$. Then $\mathfrak{q}=\mathfrak{p}$ or $\mathfrak{q}=\mathfrak{p}^2$, where $\mathfrak{p}$ is the prime below $\mathfrak{P}$. Suppose that $\mathfrak{p}\nmid\mathfrak{d}(\Lambda)$. Let $X\subseteq\Lambda$ be a finitely generated $\mathbb{Z}_L$-submodule. We say that $X$ is *isotropic modulo* $\mathfrak{q}$ if

$$\varphi(x,y)\in\mathfrak{q} \text{ for all } x,y\in X.$$

Define the *dual* of $X$ to be

$$X^{\#}=\{y\in V:\varphi(X,y)\subseteq\mathbb{Z}_L\}.$$

Then

$$\overline{\mathfrak{P}}X^{\#}=\{y\in V:\varphi(X,y)\subseteq\mathfrak{P}\}$$

and $\Lambda \cap \overline{\mathfrak{P}} X^\# \subseteq \Lambda \subset V$ is a lattice.

**Proposition 5.3.** *Let $X \subseteq \Lambda$ be isotropic modulo $\mathfrak{q}$. Then*

$$\Lambda(\mathfrak{P}, X) = \mathfrak{P}^{-1}X + (\Lambda \cap \overline{\mathfrak{P}} X^\#)$$

*is a $\mathfrak{P}^k$-neighbor of $\Lambda$, where $k = \dim X/\mathfrak{P}X$. Moreover, $\Lambda(\mathfrak{P}, X) = \Lambda(\mathfrak{P}, X')$ if and only if $X/\mathfrak{P}X = X'/\mathfrak{P}X' \subseteq \Lambda/\mathfrak{P}\Lambda$.*

*Proof.* The integrality of $\Lambda(\mathfrak{P}, X)$ is easy to verify using the fact that $\varphi(x,y) \in \mathfrak{P}\overline{\mathfrak{P}}$ for all $x, y \in X$ and $\varphi(x,y) \in \mathfrak{P}$ for all $x \in X$ and $y \in \Lambda \cap \overline{\mathfrak{P}} X^\#$.

First, we prove a claim: $\Lambda \cap \Lambda(\mathfrak{P}, X) = \Lambda \cap \overline{\mathfrak{P}} X^\#$. The inclusion ($\supseteq$) is clear. For the reverse, suppose $y \in \Lambda \cap \Lambda(\mathfrak{P}, X)$, so $y = v + w$ with $v \in \mathfrak{P}^{-1}X$ and $w \in \Lambda \cap \overline{\mathfrak{P}} X^\#$; then $v = y - w \in \Lambda$ and

$$\varphi(X, v) \subseteq \varphi(X, \mathfrak{P}^{-1}X) = \varphi(X, X)\overline{\mathfrak{P}}^{-1} \subseteq \mathfrak{P}\overline{\mathfrak{P}}\,\overline{\mathfrak{P}}^{-1} = \mathfrak{P}$$

so $v \in \Lambda \cap \overline{\mathfrak{P}} X^\#$ and thus $y = v + w \in \Lambda \cap \overline{\mathfrak{P}} X^\#$ as well. This proves the claim.

Now, choose a $\mathbb{Z}_L/\mathfrak{P}$-basis $x_1, \ldots, x_k$ for $X/\mathfrak{P}X \subseteq \Lambda/\mathfrak{P}\Lambda$. Consider the map

$$\begin{aligned} \varphi(\cdot, X) = \Lambda &\to (\mathbb{Z}_L/\overline{\mathfrak{P}})^k \\ y &\mapsto (\varphi(y, x_i)) + \overline{\mathfrak{P}}. \end{aligned}$$

Since $\mathfrak{p}$ is coprime to $\mathfrak{d}(\Lambda)$, the Hermitian form $\varphi$ is nondegenerate modulo $\overline{\mathfrak{P}}$; since $X$ is totally isotropic, it follows that $\varphi(\cdot, X)$ is surjective. Since $\varphi(y,x) = \overline{\varphi(x,y)}$ for all $x, y \in V$, we have that $\ker \varphi(\cdot, X) = \Lambda \cap \overline{\mathfrak{P}} X^\#$. Therefore, by the claim, we have

$$\Lambda/(\Lambda \cap \Lambda(\mathfrak{P}, X)) = \Lambda/(\Lambda \cap \overline{\mathfrak{P}} X^\#) \cong (\mathbb{Z}_L/\overline{\mathfrak{P}})^k. \tag{9}$$

Next, we have

$$\mathfrak{P}^{-1}X \cap \Lambda = X.$$

Therefore,

$$\begin{aligned} \Lambda(\mathfrak{P}, X)/(\Lambda \cap \Lambda(\mathfrak{P}, X)) &= (\mathfrak{P}^{-1}X + \Lambda \cap \overline{\mathfrak{P}} X^\#)/(\Lambda \cap \overline{\mathfrak{P}} X^\#) \\ &\cong \mathfrak{P}^{-1}X/(\mathfrak{P}^{-1}X \cap (\Lambda \cap \overline{\mathfrak{P}} X^\#)) \\ &= \mathfrak{P}^{-1}X/X \cong X/\mathfrak{P}X \end{aligned} \tag{10}$$

and $X/\mathfrak{P}X \cong (\mathbb{Z}_L/\mathfrak{P})^k$. Together with (9), we conclude that $\Lambda(\mathfrak{P}, X)$ is a $\mathfrak{P}^k$-neighbor.

For the final statement, if $X/\mathfrak{P}X = X'/\mathfrak{P}X'$ then it is clear that $\Lambda(\mathfrak{P}, X) = \Lambda(\mathfrak{P}, X')$ as this construction only depends on $X$ modulo $\mathfrak{P}$; the converse follows from the fact that the identification in (10) is canonical: if $\Lambda(\mathfrak{P}, X) = \Lambda(\mathfrak{P}, X')$ then $X/\mathfrak{P}X = X'/\mathfrak{P}X'$.

**Proposition 5.4.** *Let $\Pi$ be a $\mathfrak{P}^k$-neighbor of $\Lambda$. Suppose that $\mathfrak{q} = \mathfrak{P}\overline{\mathfrak{P}}$ is coprime to $\mathfrak{d}(\Lambda)$. Then there exists $X \subseteq \Lambda$ isotropic modulo $\mathfrak{P}$ with $\dim X/\mathfrak{P}X = k$ such that $\Pi = \Lambda(\mathfrak{P}, X)$.*

*Proof.* Let $X$ be the $\mathbb{Z}_L$-submodule of $\mathfrak{P}\Pi$ generated by a set of representatives for $\mathfrak{P}\Pi$ modulo $\mathfrak{P}(\Pi\cap\Lambda)$. Then $X$ is finitely generated and $\varphi(X,X)\subseteq\mathfrak{P}\overline{\mathfrak{P}}=\mathfrak{q}$ by the integrality of $\Pi$. Since $\Pi$ is a $\mathfrak{P}$-neighbor, we have

$$\Pi/(\Lambda\cap\Pi)\cong(\mathbb{Z}_L/\mathfrak{P})^k$$

so $\mathfrak{P}\Pi\subseteq\Lambda\cap\Pi\subseteq\Lambda$, showing that $X\subseteq\Lambda$ and $X/\mathfrak{P}X\cong(\mathbb{Z}_L/\mathfrak{P})^k$ by nondegeneracy.

Next, we prove that $\Pi\subseteq\Lambda(\mathfrak{P},X)$. If $y\in\Pi$, then by the integrality of $\Pi$,

$$\varphi(X,y)\subseteq\varphi(\mathfrak{P}\Pi,y)=\mathfrak{P}\varphi(\Pi,y)\subseteq\mathfrak{P}.$$

Therefore, $\Lambda\cap\Pi\subseteq\Lambda\cap\overline{\mathfrak{P}}X^{\#}$. But

$$\Lambda\cap\Pi\subsetneq\mathfrak{P}^{-1}X+\Lambda\cap\Pi\subseteq\Pi$$

and

$$\begin{aligned}(\mathfrak{P}^{-1}X+(\Lambda\cap\Pi))/(\Lambda\cap\Pi)&\cong\mathfrak{P}^{-1}X/(\mathfrak{P}^{-1}X\cap(\Lambda\cap\Pi))\\&\cong X/(X\cap\mathfrak{P}(\Lambda\cap\Pi))\cong X/\mathfrak{P}X\end{aligned}$$

by construction; since $\Pi/(\Lambda\cap\Pi)\cong(\mathbb{Z}_L/\mathfrak{P})^k$ and $X/\mathfrak{P}X\cong(\mathbb{Z}_L/\mathfrak{P})^k$, we conclude $\mathfrak{P}^{-1}X+(\Lambda\cap\Pi)=\Pi$. Thus

$$\Pi=\mathfrak{P}^{-1}X+(\Lambda\cap\Pi)\subseteq\mathfrak{P}^{-1}+(\Lambda\cap\overline{\mathfrak{P}}X^{\#})=\Lambda(\mathfrak{P},X)$$

as claimed.

But now since both $\Lambda(\mathfrak{P},X)$ and $\Pi$ are $\mathfrak{P}^k$-neighbors of $\Lambda$, they have the same invariant factors relative to $\Lambda$, so the containment $\Pi\subseteq\Lambda(\mathfrak{P},X)$ implies $\Pi=\Lambda(\mathfrak{P},X)$.

Putting together Propositions 5.3 and 5.4, we obtain the following corollary.

**Corollary 5.5.** *The map $X\mapsto\Lambda(\mathfrak{P},X)$ gives a bijection between isotropic subspaces $X\subseteq\Lambda$ modulo $\mathfrak{P}$ with $\dim X/\mathfrak{P}X=k$ and $\mathfrak{P}^k$-neighbors of $\Lambda$.*

From this corollary, we see that by taking a flag inside an isotropic subspace $X$ with $\dim X/\mathfrak{P}X=k$, every $\mathfrak{P}^k$-neighbor $\Pi$ can be obtained as a sequence

$$\Lambda_1=\Lambda(\mathfrak{P},X_1),\Lambda_2=\Lambda_1(\mathfrak{P},X_2),\ldots,\Pi=\Lambda_{k-1}(\mathfrak{P},X_{k-1})$$

of $\mathfrak{P}$-neighbors. However, not all such $k$-iterated neighbors are $\mathfrak{P}^k$-neighbors: $\Lambda$ is itself a $\mathfrak{P}$-neighbor of any of its $\mathfrak{P}$-neighbors, for example.

## *Neighbors, the genus, and strong approximation*

The $\mathfrak{P}$-neighbors can also be understood very explicitly when $\mathfrak{P}$ is *odd* (i.e., $\mathfrak{P}\nmid 2$).

Let $X \subseteq \Lambda$ be isotropic modulo $\mathfrak{P}$ with $\dim X/\mathfrak{P}X = k$. We revisit the elementary divisor theory of Section 4. There is a $\mathbb{Z}_{L,\mathfrak{p}}$-basis $x_1,\dots,x_n$ for $\Lambda_\mathfrak{p}$ such that $x_1,\dots,x_k$ is a basis for $X_\mathfrak{p}$ such that a basis for $\Lambda(\mathfrak{P},X)_\mathfrak{p}$ is

$$(\overline{P}/P)x_1,\dots,(\overline{P}/P)x_k,x_{k+1},\dots,x_n$$

if $\mathfrak{P} \neq \overline{\mathfrak{P}}$ and is

$$Px_1,\dots,Px_k,x_{k+1},\dots,x_{n-k},P^{-1}x_{n-k+1},\dots,P^{-1}x_n,$$

if $\mathfrak{P} = \overline{\mathfrak{P}}$, where $P$ is a uniformizer of $\mathfrak{P}$. In the first case, since $q = \overline{P}P^{-1}$ has $q\overline{q} = 1$, this diagonal change of basis is an isometry and thus $\Lambda(\mathfrak{P},X)_\mathfrak{p} \cong \Lambda_\mathfrak{p}$; a direct calculation in the latter case shows again that it is an isometry.

Since the invariant factors of a $\mathfrak{P}^k$-neighbor are supported over $\mathfrak{p}$, we have proven the following lemma.

**Lemma 5.6.** *Let $\Pi$ be a $\mathfrak{P}$-neighbor of $\Lambda$ with $\mathfrak{p}$ below $\mathfrak{P}$ and $\mathfrak{p} \nmid \mathfrak{d}(\Lambda)$. Suppose that $\mathfrak{p}$ is odd. Then $\Pi$ belongs to the genus of $\Lambda$.*

Now we form the graph of $\mathfrak{P}^k$-neighbors: the vertices consist of a set of equivalence classes of lattices in the genus of $\Lambda$, and for each vertex $\Pi$ we draw a directed edge to the equivalence class of each $\mathfrak{P}^k$-neighbor of $\Pi$. This graph is $\kappa$-regular, where $\kappa$ is the number of isotropic subspaces of $\Lambda_\mathfrak{p}$ modulo $\mathfrak{P}$ of dimension $k$—since all lattices in the genus are isomorphic. If, for example, $\varphi$ is the standard form (so is totally split) and $\mathfrak{P} \neq \overline{\mathfrak{P}}$, then this number is simply the cardinality of the Grassmanian $\mathrm{Gr}(n,k)(\mathbb{F}_\mathfrak{P})$ of subspaces of dimension $k$ in a space of dimension $n$, and we have the formula

$$\#\mathrm{Gr}(n,k)(\mathbb{F}_q) = \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})}. \tag{11}$$

To conclude, we show that in fact the entire genus can be obtained via iterated $\mathfrak{P}$-neighbors; this is equivalent to the assertion that the graph of $\mathfrak{P}$-neighbors is connected.

First, we need the following important result, a consequence of strong approximation. For the orthogonal case $L = F$, see Eichler [16], Kneser [34], or O'Meara [41, §104]; for the unitary case $L/F$, see Shimura [48, Theorem 5.24, 5.27] (and Schiemann [45, Theorem 2.10]); and for a further perspectives, see the survey by Kneser [35].

We say that a lattice $\Lambda$ is *nice at the ramified primes* if for all $\mathfrak{q}$ ramified in $L/F$, the lattice $\Lambda_\mathfrak{q}$ splits a one-dimensional sublattice. If $n$ is odd or $L = F$ or $\Lambda$ is even unimodular, this condition holds.

Let $\mathrm{Cl}(\mathbb{Z}_L)$ be the class group of $\mathbb{Z}_L$ and let $\mathrm{Cl}(\mathbb{Z}_L)^{\langle\neg\rangle}$ be the set of those classes that have a representative $\mathfrak{A}$ with $\mathfrak{A} = \overline{\mathfrak{A}}$. Note $\mathrm{Cl}(\mathbb{Z}_L) = \mathrm{Cl}(\mathbb{Z}_L)^{\langle\neg\rangle}$ if $L = F$.

**Theorem 5.7 (Strong approximation).** *Suppose that*

(i) *$L = F$, $n \geq 3$, and $\mathfrak{d}(\Lambda)$ is squarefree, or*

(ii) $[L:F]=2$, $n\geq 2$, *and* $\Lambda$ *is nice at the ramified primes.*

*Let $S$ be a nonempty set of primes of $L$ coprime to $\mathfrak{d}(\Lambda)$ that represent all elements in* $\mathrm{Cl}(\mathbb{Z}_L)/\mathrm{Cl}(\mathbb{Z}_L)^{\langle\overline{\ }\rangle}$.

*Then every lattice in* $\mathrm{gen}(\Lambda)$ *is equivalent to a lattice $\Pi$ with $\Pi_{\mathfrak{q}}=\Lambda_{\mathfrak{q}}$ for all primes $\mathfrak{q}$ below a prime $\mathfrak{Q}\notin S$.*

*Proof (sketch).* The hypotheses $n\geq 3$ and $n\geq 2$ are necessary, as they imply that the corresponding spin or special unitary group is simply connected; they also further imply that for all primes $\mathfrak{p}\nmid\mathfrak{d}(\Lambda)$ below a prime $\mathfrak{P}\in S$, the form $\varphi_{\mathfrak{p}}$ on $V_{\mathfrak{p}}$ is isotropic, so $G_{\mathfrak{p}}$ is not compact. Since the set $S$ is nonempty, strong approximation then implies that every lattice in the spin genus or special genus of $\Lambda$ is equivalent to a lattice $\Pi$ as in the statement of the theorem. Finally, the hypothesis that $\mathfrak{d}(\Lambda)$ is squarefree in the orthogonal case implies that the genus of $\Lambda$ contains only one spinor genus (see O'Meara [41, §102] or Kneser [33]); and the difference between the special genus and the genus of $\Lambda$ is measured by the group $\mathrm{Cl}(\mathbb{Z}_L)/\mathrm{Cl}(\mathbb{Z}_L)^{\langle\overline{\ }\rangle}$ by work of Shimura when $\Lambda$ is nice at the ramified primes.

*Remark 5.8.* These are not the minimal set of hypotheses in which strong approximation holds, but they will suffice for our purposes; see the references above for a more comprehensive treatment.

We then have the following corollary; see also Kneser [34, §2], Iyanaga [28, 2.8–2.11], and Hoffmann [24, Theorem 4.7].

**Corollary 5.9.** *Under the hypotheses of Theorem* 5.7*, every lattice in* $\mathrm{gen}(\Lambda)$ *can be obtained as a sequence of $\mathfrak{P}$-neighbors for $\mathfrak{P}\in S$.*

*Proof.* Let $\Pi\in\mathrm{gen}(\Lambda)$. By strong approximation, we may assume that $\Pi_{\mathfrak{Q}}=\Lambda_{\mathfrak{Q}}$ for all $\mathfrak{Q}\notin S$.

First, suppose that $\Pi_{\mathfrak{Q}}=\Lambda_{\mathfrak{Q}}$ for all $\mathfrak{Q}\neq\mathfrak{P}$. Then $\mathfrak{P}^m\Pi\subseteq\Lambda$ for some $m\in\mathbb{Z}_{\geq 0}$. We proceed by induction on $m$. If $m=0$, then $\Pi\subseteq\Lambda$ and since $\mathfrak{d}(\Pi)=\mathfrak{d}(\Lambda)$ we have $\Pi=\Lambda$.

Suppose $m>0$, and choose $m$ minimal so that $\mathfrak{P}^m\Pi\subseteq\Lambda$. Let $X$ be the $\mathbb{Z}_L$-submodule of $\mathfrak{P}^m\Pi$ generated by a set of representatives for $\mathfrak{P}^m\Pi$ modulo $\mathfrak{P}^m\Pi\cap\mathfrak{P}\Lambda$. Then $X\subseteq\mathfrak{P}^m\Pi\subseteq\Lambda$. Now consider again the proof of Proposition 5.4. We see that $X$ is isotropic (in fact, $\varphi(X,X)\in\mathfrak{q}^m$). Form the neighbor $\Lambda(\mathfrak{P},X)$. Then $\Lambda(\mathfrak{P},X)$ can be obtained from a sequence of $\mathfrak{P}$-neighbors of $\Lambda$.

Now we have

$$\mathfrak{P}^{m-1}\Pi=\mathfrak{P}^{-1}X+(\Lambda\cap\mathfrak{P}^{m-1}\Pi)\subseteq\mathfrak{P}^{-1}X+(\Lambda\cap\overline{\mathfrak{P}}X^{\#})=\Lambda(\mathfrak{P},X)$$

since

$$\varphi(X,\mathfrak{P}^{m-1}\Pi)\subseteq\varphi(\mathfrak{P}^m\Pi,\mathfrak{P}^{m-1}\Pi)\subseteq\mathfrak{P}\mathfrak{q}^{m-1}\varphi(\Pi,\Pi)\subseteq\mathfrak{P}.$$

Therefore, by induction, $\mathfrak{P}^{m-1}\Pi$ can be obtained by a repeated $\mathfrak{P}$-neighbor of $\Lambda(\mathfrak{P},X)$, and we are done by transitivity.

In the general case, we simply repeat this argument for each prime $\mathfrak{P}$ in $\mathbb{Z}_L$.

### *Hecke operators*

We now connect the theory of neighbors to Hecke operators via elementary divisors and the Cartan decomposition as in the previous section. Specifically, we compute the action of $\mathscr{H}(\mathsf{G}(F_\mathfrak{p}),K_\mathfrak{p})$ on $M(W,\widehat{K})$ for primes $\mathfrak{p}\nmid\mathfrak{d}(\Lambda)$. In this case, the corresponding lattice is unimodular.

As should now be evident from this description in terms of maximal isotropic subspaces, the Hecke operator acts on a lattice by a summation over its neighbors. We record this in the following theorem.

**Theorem 5.10.** *Let $\widehat{p}\in\widehat{G}$ correspond to the sequence*

$$0\le\cdots\le 0\le\underbrace{1\le\cdots\le 1}_{k}$$

*in Proposition 4.4 or 4.3. Write $\widehat{K}\widehat{p}\widehat{K}=\bigsqcup\widehat{p}_j\widehat{K}$. Then for any $\widehat{x}\in\widehat{G}$, the set of lattices*

$$\Pi_j=\widehat{x}\widehat{p}_j\Lambda=\widehat{x}\widehat{p}_j\widehat{\Lambda}\cap V$$

*is in bijection with the set of $\mathfrak{P}^k$-neighbors of $\widehat{x}\Lambda$.*

*Proof.* Each $\Pi_j$ is indeed a $\mathfrak{P}^k$-neighbor, as is visible by looking at the corresponding invariant factors. Since the $\mathfrak{P}^k$-neighbors are in bijection with maximal isotropic subspaces and so are the cosets $\widehat{p}_j$, these sets are in bijection.

## 6 Algorithmic details

Having discussed the theory in the previous sections, we now present our algorithm for using lattices to compute algebraic modular forms.

### *General case*

We first give a general formulation for algebraic groups: this general blueprint can be followed in other situations (including symplectic groups, exceptional groups, etc.). We compute the space $M(W,\widehat{K})$ of algebraic modular forms of weight $W$ and level $\widehat{K}$ on a group $\mathsf{G}$. To begin with, we must decide upon a way to represent in bits the group $\mathsf{G}$, the open compact subgroup $\widehat{K}$, and the $G$-representation $W$ so we can work explicitly with these objects. Then, to compute the space $M(W,\widehat{K})$ as a module for the Hecke operators, we carry out the following tasks:

1. Compute representatives $\widehat{x}_i\widehat{K}$ ($i=1,\dots,h$) for $G\backslash\widehat{G}/\widehat{K}$, as in (2), compute $\Gamma_i=G\cap\widehat{x}_i\widehat{K}\widehat{x}_i^{-1}$, and initialize

$$H = \bigoplus_{i=1}^{h} H^0(\Gamma_i, W).$$

Choose a basis of (characteristic) functions $f$ of $H$.

2. Determine a set of Hecke operators $T(\widehat{p})$ that generate $\mathscr{H}(\widehat{K})$, as in Section 4. For each such $T(\widehat{p})$:

   a. Decompose the double coset $\widehat{K}\widehat{p}\widehat{K}$ into a union of right cosets $\widehat{p}_j\widehat{K}$, as in (3);
   b. For each $\widehat{x}_i$ and $\widehat{p}_j$, find $\gamma_{ij} \in G$ and $j^*$ so that

$$\widehat{x}_i\widehat{p}_j\widehat{K} = \gamma_{ij}\widehat{x}_{j^*}\widehat{K}.$$

   c. Return the matrix of $T(\widehat{p})$ acting on $H$ via the formula

$$(T(\widehat{p})f)(\widehat{x}_i) = \sum_j \gamma_{ij} f_m(\widehat{x}_{j^*})$$

   for each $f$ in the basis of $H$.

In step 2c, since each function $f_m$ is a characteristic function, we are simply recording for each occurrence of $j^*$ an element of $G$.

We now turn to each of the pieces of this general formulation in our case.

## *Representation in bits*

We follow the usual algorithmic conventions for number fields [5]. A Hermitian form $(V, \varphi)$ for $L/F$ is represented by its Gram matrix. We represent a $\mathbb{Z}_F$-lattice $\Lambda \subset V$ by a *pseudobasis* over $\mathbb{Z}_F$, writing

$$\Lambda = \mathfrak{A}_1 x_1 \oplus \cdots \oplus \mathfrak{A}_n x_n$$

with $x_1, \ldots, x_n \in V$ linearly independent elements and $\mathfrak{A}_i \subset L$ fractional $\mathbb{Z}_L$-ideals [6]. The open compact subgroup $\widehat{K}$ is the stabilizer of $\Lambda$ by (8) so no further specification is required.

The irreducible, finite dimensional representations of $G$ are given by highest weight representations. The theory is explained e.g. by Fulton and Harris [19], and in Magma there is a construction of these representations [13, 4], based on the LiE system [38].

### *Step 1: Enumerating the set of representatives*

We enumerate a set of representatives $\widehat{x}_i\widehat{K}$ for $G\backslash\widehat{G}/\widehat{K}$ using the results of Sections 4 and 5. For this, we will use Corollary 5.9, and so we must assume the hypotheses of Theorem 5.7, namely:

(i) $L = F$, $n \geq 3$, and $\mathfrak{d}(\Lambda)$ is squarefree, or
(ii) $[L : F] = 2$, $n \geq 2$, and $\Lambda$ is nice at the ramified primes.

Next, according to Corollary 5.9 we compute a nonempty set of primes $S$ of $L$ coprime to $2\mathfrak{d}(\Lambda)$ that represent all elements in $\mathrm{Cl}(\mathbb{Z}_L)/\mathrm{Cl}(\mathbb{Z}_L)^{\langle -\rangle}$. By the Chebotarev density theorem, we may assume that each prime $\mathfrak{P}$ is split in $L/F$ if $L \neq F$. There are standard techniques for computing the class group due to Buchmann (see Cohen [6, Algorithm 6.5.9] for further detail). We compute the action of the involution $\overline{\ }$ on $\mathrm{Cl}(\mathbb{Z}_L)$ directly and then compute the subgroup $\mathrm{Cl}(\mathbb{Z}_L)^{\langle -\rangle}$ fixed by $\overline{\ }$ and the corresponding quotient using linear algebra over $\mathbb{Z}$.

Next, we traverse the graph of $\mathfrak{P}$-neighbors for each $\mathfrak{P} \in S$. To do this, we perform the following tasks:

a. Compute a basis for $\Lambda_{\mathfrak{P}}$ as in Propositions 4.3 and 4.4 according as $L = F$ or $L \neq F$.
b. Compute the one-dimensional isotropic subspaces modulo $\mathfrak{P}$ in terms of the basis $e_i$ for the maximal isotropic subspace.
c. For each such subspace $X$, compute the $\mathfrak{P}$-neighbor $\Lambda(\mathfrak{P}, X) = \mathfrak{P}^{-1}X + \overline{\mathfrak{P}}X^{\#}$ using linear algebra.
d. Test each neighbor $\Lambda(\mathfrak{P}, X)$ for isometry against the list of lattices already computed. For each new lattice $\Lambda'$, repeat and return to step a with $\Lambda'$ in place of $\Lambda$.

Since the genus is finite, this algorithm will terminate after finitely many steps.

*Remark 6.1.* One can also use the exact mass formula of Gan and Yu [21] and Gan, Hanke, and Yu [20] as a stopping criterion, or instead as a way to verify the correctness of the output.

Further comments on each of these steps.

First, in steps 1a–1b we compute a basis. When $[L : F] = 2$, this is carried out as in Section 5 via the splitting $L_{\mathfrak{p}} \cong F_{\mathfrak{p}} \times F_{\mathfrak{p}}$. When $L = F$, we use standard methods including diagonalization of the quadratic form: see e.g. work of the second author [51] and the references therein, including an algorithm for the normalized form of a quadratic form over a dyadic field, which at present we exclude. From the diagonalization, we can read off the maximal isotropic subspace, and this can be computed by working not over the completion but over $\mathbb{Z}_F/\mathfrak{p}^e$ for a large $e$. Next, in step 1c we compute the neighbors. This is linear algebra. Step 1d, isometry testing, is an important piece in its own right, which we discuss in the next subsection; as a consequence of this discussion, we will also compute $\Gamma_i = \mathrm{Aut}(\Lambda_i)$. From this, the computation of a basis for $H = \bigoplus_{i=1}^{h} H^0(\Gamma_i, W)$ is straightforward.

### *Isometry testing*

To test for isometry, we rely on standard algorithms for quadratic $\mathbb{Q}$-spaces and $\mathbb{Z}$-lattices even when computing relative to a totally real base field $F$ or a CM extension $L/F$. Let $a_1,\dots,a_d$ be a $\mathbb{Z}$-basis for $\mathbb{Z}_L$ with $a_1 = 1$, and let $x_1,\dots,x_n$ be a basis of $V$. Then

$$\{a_i x_j\}_{\substack{i=1,\dots,d \\ j=1,\dots,n}}$$

is a $\mathbb{Q}$-basis of $V$. Define $\mathbb{Q}$-bilinear pairings

$$\varphi_i : V \times V \longrightarrow \mathbb{Q} \quad \text{by} \quad \varphi_i(x,y) = \mathrm{tr}_{L/\mathbb{Q}}\, \varphi(a_i x, y).$$

Since $a_1 = 1$ and $\varphi$ is a definite Hermitian form on $V$ over $L$, $\varphi_1$ is a positive definite, symmetric, bilinear form on $V$ over $\mathbb{Q}$. In other words, $(V,\varphi_1)$ is a quadratic $\mathbb{Q}$-space. The $L$-space $(V,\varphi)$ can be explicitly recovered from $(V,\varphi_1)$, together with the extra data $\varphi_2,\dots,\varphi_d$ by linear algebra. Note that the forms $\varphi_2,\dots,\varphi_d$ are in general neither symmetric nor positive definite.

**Lemma 6.2.** *Let $\Lambda$ and $\Pi$ be lattices in $V$. A $\mathbb{Z}$-linear map $f : \Lambda \to \Pi$ is an $\mathbb{Z}_L$-linear isometry if and only if each $\varphi_i$ is invariant under $f$.*

Using Lemma 6.2, we reduce the problem of testing if two Hermitian lattices over $\mathbb{Z}_F$ are isometric to a problem of testing if two lattices over $\mathbb{Z}$ are isometric in a way which preserves each $\varphi_i$. For this, we rely on the algorithm of Plesken and Souvignier [43], which matches up short vectors and uses other tricks to rule out isometry as early as possible, and has been implemented in Magma [2] by Souvignier, with further refinements by Steel, Nebe, and others.

For each representative lattice found, we compute a set of invariants to quickly rule out isometry whenever possible. These invariants include things like the sizes of the automorphism groups, the first few terms in the theta series, and invariants of sublattices (e.g. those generated by short vectors).

*Remark 6.3.* An essential speed up in the case of Brandt modules is given by Dembélé and Donnelly [10] (see also Kirschmer and the second author [31, Algorithm 6.3]). To decide if two right ideals $I, J$ in a quaternion order $\mathcal{O}$ are isomorphic, one first considers the colon ideal $(I : J)_L = \{\alpha \in B : \alpha J \subseteq I\}$ to reduce the problem to show that a single right ideal is principal; then one scales the positive definite quadratic form over $\mathbb{Q}$ by an explicit factor to reduce the problem to a single shortest vector calculation. It would be very interesting to find an analogue of this trick in this context as well.

### *Step 2: Hecke operators*

Essentially all of the work to compute Hecke operators has already been set up in enumerating the genus in Step 1. The determination of the Hecke operators follows

from Sections 4 and 5, and their explicit realization is the same as in Step 1a. We work with those Hecke operators supported at a single prime. In Step 2a, from Theorem 5.10, the double coset decomposition is the same as set of $\mathfrak{P}$-neighbors, which we compute as in Step 1. In Step 2b, we compute the isometry $\gamma_{ij}$ using isometry testing as in the previous subsection: we quickly rule out invalid candidates until the correct one is found, and find the corresponding isometry. Finally, in Step 2c, we collect the results by explicit computations in the weight representation.

## 7 Examples

In this section, we illustrate our methods by presenting the results of some explicit computations for groups of the form $\mathsf{G} = \mathsf{U}_{L/F}(3)$, relative to a CM extension $L/F$, where $L$ has degree 2, 4, or 6. We compute the Hecke operator at unramified, degree one primes $\mathfrak{p}$ of $L$ corresponding to summing over $\mathfrak{p}$-neighbours of a lattice.

*Remark 7.1.* We made several checks to ensure the correctness of our programs. First, we checked that matrices of Hecke operators for $\mathfrak{p}$ and $\mathfrak{q}$ with $\mathfrak{p} \neq \mathfrak{q}$ commuted. (They did.) Additionally, a known instance of Langlands functoriality implies that forms on $U(1) \times U(1) \times U(1)$ transfer to $U(3)$. Checking that resulting endoscopic forms occur in the appropriate spaces [39, §§4.2, 4.6] also provided a useful test of our implementation. (It passed.)

*Example 7.2.* $U_{L/F}(3)$, $L = \mathbb{Q}(\sqrt{-7})$, $F = \mathbb{Q}$, weights $(0,0,0)$ and $(3,3,0)$:

**Table 1** Computation of $T_{\mathfrak{p},1}$ on $M(\mathbb{Q})$ for unramified, degree one $\mathfrak{p} \subset \mathbb{Z}_L$ with $2 < N(\mathfrak{p}) < 200$.

| $N(\mathfrak{p})$ | 2 | 11 | 23 | 29 | 37 | 43 | 53 | 67 | 71 | 79 | 107 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| time (s) | 0.02 | 0.07 | 0.18 | 0.28 | 0.42 | 0.57 | 0.82 | 1.35 | 1.46 | 1.86 | 3.73 |
| $a_p$ | 7 | 133 | 553 | 871 | 1407 | 1893 | 2863 | 4557 | 5113 | 6321 | 11557 |
| $b_p$ | -1 | 5 | 41 | -25 | -1 | 101 | 47 | -51 | 185 | -15 | 293 |
| | | | | | | | | | | | |
| $N(\mathfrak{p})$ | 109 | 113 | 127 | 137 | 149 | 151 | 163 | 179 | 191 | 193 | 197 |
| time (s) | 4.18 | 4.59 | 5.85 | 7.08 | 8.56 | 9.04 | 10.88 | 13.78 | 16.92 | 17.22 | 17.29 |
| $a_p$ | 11991 | 12883 | 16257 | 18907 | 22351 | 22953 | 26733 | 32221 | 36673 | 37443 | 39007 |
| $b_p$ | 215 | -109 | 129 | -37 | 335 | 425 | 237 | -163 | -127 | 131 | 479 |

Here, we extend aspects of the calculation in the principal example of [39]. In this case, the class number of the principal genus of rank 3 Hermitian lattices for $L/\mathbb{Q}$ is 2, with classes represented by the standard lattice $\Lambda_1 = \mathbb{Z}_L^3$ and the lattice $\Lambda_2 \subset L^3$ with basis

$$(1-\omega,0,0), \quad (1,1,0), \quad \tfrac{1}{2}(-3+\omega,-1+\omega,-1+\omega). \qquad \left(\omega = \tfrac{1}{2}(1+\sqrt{-7})\right)$$

The lattices $\Lambda_1$ and $\Lambda_2$ are 2-neighbours:

$$\omega\Lambda_2 \subset \Lambda_1, \quad \bar{\omega}\Lambda_1 \subset \Lambda_2.$$

(Representatives for the ideal classes in the principal genus were computed in the first place by constructing the 2-neighbour graph $\Lambda_1$.) It follows that the space of $M(\mathbb{Q})$ of algebraic modular forms for $U_{L/F}(3)$ with trivial coefficients is simply the 2-dimensional space of $\mathbb{Q}$-valued function on $\{[\Lambda_1],[\Lambda_2]\}$. We obtain two distinct systems $a_\mathfrak{p}$ and $b_\mathfrak{p}$ of Hecke eigenvalues occurring in $M(\mathbb{Q})$. (See Table 1.) We point out observations of Loeffler considering the nature of the corresponding algebraic modular forms: First, observe that the system $a_\mathfrak{p}$ is "Eisenstein", in the sense that the eigenvalues of $T_{\mathfrak{p},1}$ is the degree of the Hecke operator $T_{\mathfrak{p},1}$:

$$a_\mathfrak{p} = N(\mathfrak{p})^2 + N(\mathfrak{p}) + 1.$$

Equivalently, the corresponding algebraic modular form is the lift from $U(1) \times U(1) \times U(1)$ of $\chi_{\text{triv}} \times \chi_{\text{triv}} \times \chi_{\text{triv}}$. The algebraic modular form with system of eigenvalues $b_\mathfrak{p}$ is also a lift form $U(1) \times U(1) \times U(1)$:

$$b_\mathfrak{p} = \mathfrak{p}^2 + \mathfrak{p}\bar{\mathfrak{p}} + \bar{\mathfrak{p}}^2.$$

Here, we abuse notation and write $\mathfrak{p}$ for either of its generators, and note that the expression on the right in the above is independent of this choice.

We now consider analogous computations involving forms of higher weight. The space $M(V_{3,3,0})$ the associated to the above data has dimension 4, while the representation space $V_{3,3,0}$ itself has dimension 64. Loeffler [39] showed that $M(V_{3,3,0})$ splits as the direct sum of two 2-dimensional, Hecke-stable subspaces not diagonalizable over $\mathbb{Q}(\sqrt{-7})$:

$$M(V_{3,3,0}) = W_1 \oplus W_2.$$

One of these spaces arises as the lift involving a 2-dimensional Galois conjugacy class of classical eigenforms in $S_9(\Gamma_1(7))$ via a lifting from the endoscopic subgroup $U(1) \times U(2)$ of $U(3)$. The other corresponds to a Galois conjugacy class of nonendoscopic forms, whose associated $\ell$-adic Galois representations $\rho : G_L \to GL_2(\mathbb{Q}_\ell)$ are irreducible.

We consider the corresponding modular space $M(V_{3,3,0}/\mathbb{F}_7)$ of mod $(\sqrt{-7})$-modular forms of weight $(3,3,0)$. We computed the Hecke operators $T_{\mathfrak{p},1}$ for unramified, degree one primes $\mathfrak{p} \subset \mathbb{Z}_L$ of norm at most 100. In Table 2, we present the corresponding run-times.

Simultaneously diagonalizing the matrices of these Hecke operators we obtain two mod $(\sqrt{-7})$ systems of eigenvalues that we write $\bar{a}_\mathfrak{p}$ and $\bar{b}_\mathfrak{p}$. We choose this notation because those systems are the reductions modulo 7 of the corresponding trivial weight systems $a_\mathfrak{p}$ and $b_\mathfrak{p}$ from earlier. We have an explicit modulo 7 congruence between a nonendoscopic form in weight $(3,3,0)$ and an endoscopic form in weight $(0,0,0)$. Thus, the modulo 7 Galois representation associated to the system $\bar{b}_\mathfrak{p}$ is reducible.

**Table 2** Computation of $T_{\mathfrak{p},1}$ mod $(\sqrt{-7})$ for degree one, unramified $\mathfrak{p} \subset \mathbb{Z}_L$ with $2 < N(\mathfrak{p}) < 100$.

| | 2 | 11 | 23 | 29 | 37 | 43 | 53 | 67 | 71 | 79 |
|---|---|---|---|---|---|---|---|---|---|---|
| Steps 2a,b | 0.11 | 2.49 | 12.37 | 26.52 | 60.08 | 128.29 | 265.47 | 595.90 | 984.19 | 1561.67 |
| Step 2c | 0.41 | 26.77 | 123.82 | 208.38 | 328.95 | 450.68 | 686.25 | 1431.75 | 1414.790 | 1774.52 |
| $\bar{a}_{\mathfrak{p}}$ | 0 | 0 | 0 | 3 | 0 | 3 | 0 | 0 | 3 | 0 |
| $b_{\mathfrak{p}}$ | 6 | 5 | 6 | 3 | 6 | 3 | 5 | 5 | 3 | 6 |

*Example 7.3.* $U_{L/F}(3)$, $F = \mathbb{Q}(\sqrt{13})$, $L = F\left(\sqrt{-13-2\sqrt{13}}\right)$, weight (0,0,0):

In this example, the class number of the principal genus is 9, as is the dimension of the corresponding space of automorphic forms with trivial weight. We computed

**Table 3** Computation of $T_{\mathfrak{p},1}$ for degree one, unramified $\mathfrak{p} \subset \mathbb{Z}_L$ with $2 < N(\mathfrak{p}) < 250$.

| $N(\mathfrak{p})$ | 29 | 53 | 61 | 79 | 107 | 113 | 131 | 139 | 157 | 191 | 211 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| time (s) | 15.15 | 51.73 | 70.35 | 123.21 | 216.82 | 242.20 | 339.50 | 378.81 | 486.22 | 727.81 | 943.89 |
| $\bar{a}_{\mathfrak{p}}$ | 4 | 11 | 12 | 5 | 5 | 3 | 6 | 10 | 1 | 11 | 2 |

the matrices of the Hecke operators acting on the $\mathbb{Q}$-vector space $M(\mathbb{Q})$ for unramified, degree one $\mathfrak{p} \subset \mathbb{Z}_L$ with $2 < N(\mathfrak{p}) < 250$. There appears to be a 1-dimensional "Eisenstein" subspace on which $T_{\mathfrak{p},1}$ acts via $\deg T_{\mathfrak{p},1} = N(\mathfrak{p})^2 + N(\mathfrak{p}) + 1$. The 8-dimensional complement of this line decomposes into $\mathbb{Q}$-irreducible subspaces of dimensions 2, 2, and 4. In all of these computations, the level subgroup is the stabilizer of the standard lattice $\mathbb{Z}_L^3 \subset L^3$.

The Hecke algebra does acts nonsemisimply on the space $M(\mathbb{F}_{13})$ of modulo 13 automorphic forms. It appears that the minimal polynomial of $T_{\mathfrak{p},1}$ has degree 6 when $N(\mathfrak{p}) \equiv 1 \pmod{13}$ and degree 7 when $N(\mathfrak{p}) \equiv 3, 9 \pmod{13}$. (Other residue classes do not occur for norms of degree one primes of $F$ splitting in $L$.) When $N(\mathfrak{p}) \equiv 1 \pmod{13}$, the eigenvalue $3 \equiv N(\mathfrak{p})^2 + N(\mathfrak{p}) + 1 \pmod{13}$ occurs with multiplicity 5, while when $N(\mathfrak{p}) \equiv 3, 9 \pmod{13}$, the eigenvalue $0 \equiv N(\mathfrak{p})^2 + N(\mathfrak{p}) + 1 \pmod{13}$ occurs with multiplicity 1. Finally, is a 1-dimensional eigenspace in $M(\mathbb{F}_{13})$ with eigenvalues $\bar{a}_q$ as in Table 3.

*Example 7.4.* $U_{L/F}(3)$, $K = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$, $L = \mathbb{Q}(\zeta_7)$, weight $(0,0,0)$:

In this case, the class number of the principal genus is 2, with the classes represented by the standard lattice $\Lambda_1 = \mathbb{Z}_L^3$ and its 29-neighbour $\Lambda_2$ with basis

$$\begin{aligned}(\zeta_7 + \zeta_7^4 - \zeta_7^5, 0, 0), \quad & (6,1,0), \\ & \tfrac{1}{29}(-138 - 234\zeta_7 - 210\zeta^2 - 303\zeta^3 - 258\zeta^4 - 117\zeta^5, \\ & \qquad 16 + 12\zeta + 13\zeta^2 + 20\zeta^3 + 11\zeta^4 + 6\zeta^5, \\ & \qquad\qquad 16 + 12\zeta + 13\zeta^2 + 20\zeta^3 + 11\zeta^4 + 6\zeta^5).\end{aligned}$$

(This calculation took 1.85 seconds.)

**Table 4** Timings: computation of $T_{\mathfrak{p},1} \bmod (\sqrt{-7})$ for $\mathfrak{p}$ with $2 < N(\mathfrak{p}) < 100$ and $\mathfrak{p} \neq \bar{\mathfrak{p}}$

| $N(\mathfrak{p})$ | 29 | 43 | 71 | 113 | 127 | 197 | 211 | 239 | 281 |
|---|---|---|---|---|---|---|---|---|---|
| time (s) | 2.16 | 2.85 | 6.77 | 16.43 | 21.35 | 51.14 | 53.58 | 73.05 | 101.84 |
| $a_{\mathfrak{p}}$ | 871 | 1893 | 5113 | 12883 | 16257 | 39007 | 44733 | 57361 | 79243 |
| $b_{\mathfrak{p}}$ | -25 | 101 | 185 | -109 | 129 | 479 | -67 | 17 | 395 |

Automorphism groups of $\Lambda_1$ and $\Lambda_2$ and their roles in this computation. As above, $a_{\mathfrak{p}} = N(\mathfrak{p})^2 + N(\mathfrak{p}) + 1 = \deg T_{\mathfrak{p},1}$, and the form with system of Hecke eigenvalues $a_{\mathfrak{p}}$ is a lift from $U(1) \times U(1) \times U(1)$. Also, observe that

$$a_{\mathfrak{p}} \equiv b_{\mathfrak{p}} \equiv 3 \pmod 7,$$

implying that the modulo 7 Galois representation attached to the system $b_{\mathfrak{p}}$ is reducible.

**Acknowledgements** The authors would like to thank Lassina Dembélé and David Loeffler for helpful conversations.

## References

1. Armand Borel, *Linear algebraic groups*, second enlarged ed., Graduate Texts in Math., vol. 126, Springer-Verlag, New York, 1991.
2. Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), vol. 3–4, 235–265.
3. Sarah Chisholm, *Lattice methods for algebraic modular forms on quaternionic unitary groups*, Ph.D. thesis, University of Calgary, anticipated 2013.
4. Arjeh M. Cohen, Scott H. Murray, and D. E. Taylor, *Computing in groups of Lie type*, Math. Comp. **73** (2004), no. 247, 1477–1498.
5. Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Math., vol. 138, Springer-Verlag, Berlin, 1993.
6. Henri Cohen, *Advanced topics in computational algebraic number theory*, Graduate Texts in Math., vol. 193, Springer-Verlag, Berlin, 2000.
7. Clifton Cunningham and Lassina Dembélé, *Computation of genus 2 Hilbert-Siegel modular forms on $\mathbb{Q}(\sqrt{5})$ via the Jacquet-Langlands Correspondence*, Experimental Math. **18** (2009), no. 3, 337–345.
8. Lassina Dembélé, *Quaternionic Manin symbols, Brandt matrices and Hilbert modular forms*, Math. Comp. **76** (2007), no. 258, 1039–1057.
9. Lassina Dembélé, *A non-solvable Galois extension of $\mathbb{Q}$ ramified at 2 only*, C. R. Acad. Sci. Paris, Ser. I, **347** (2009), 111–116.
10. Lassina Dembélé and Steve Donnelly, *Computing Hilbert modular forms over fields with non-trivial class group*, Algorithmic number theory (Banff, 2008), Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, 371–386.
11. Lassine Dembélé, Matthew Greenberg, and John Voight, *Nonsolvable number fields ramified only at 3 and 5*, Compositio Math. **149** (2011), no. 3, 716–734.

12. Lassina Dembélé and John Voight, *Explicit methods for Hilbert modular forms*, accepted to Elliptic curves, Hilbert modular forms and Galois deformations.
13. W. A. de Graaf, *Constructing representations of split semisimple Lie algebras*, J. Pure Appl. Algebra, Effective methods in algebraic geometry (Bath, 2000), **164** (2001), no. 1–2, 87–107.
14. Luis Dieulefait, *A non-solvable extension of* $\mathbb{Q}$ *unramified outside 7*, to appear in Compositio Math.
15. Martin Eichler, *On theta functions of real algebraic number fields*, Acta Arith. **33** (1977), no. 3, 269–292.
16. Martin Eichler, *Quadratische Formen und orthogonale Gruppen*, Springer-Verlag, Berlin, 1952.
17. Martin Eichler, *The basis problem for modular forms and the traces of the Hecke operators*, Modular functions of one variable, I (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Lecture Notes in Math., vol. 320, Springer, Berlin, 1973, 75–151.
18. Martin Eichler, *Correction to: "The basis problem for modular forms and the traces of the Hecke operators"*, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Lecture Notes in Math., vol. 476, Springer, Berlin, 1975, 145–147.
19. William Fulton and Joe Harris, *Representation theory: a first course*, Graduate Texts in Math., vol. 129, Springer-Verlag, New York, 1991.
20. Wee Teck Gan, Jonathan Hanke, and Jiu-Kang Yu, *On an exact mass formula of Shimura*, Duke Math. J. **107** (2001), no. 1, 103–133.
21. Wee Teck Gan and Jiu-Kang Yu, *Group schemes and local densities*, Duke Math. J. **105** (2000), no. 3, 497–524.
22. Matt Greenberg and John Voight, *Computing systems of Hecke eigenvalues associated to Hilbert modular forms*, Math. Comp. **80** (2011), 1071–1092.
23. Benedict Gross, *Algebraic modular forms*, Israel J. Math. **113** (1999), 61–93.
24. Detlev W. Hoffmann, *On positive definite Hermitian forms*, Manuscripta Math. **71** (1991), 399–429.
25. Hiroaki Hijikata, Arnold K. Pizer, and Thomas R. Shemanske, *The basis problem for modular forms on* $\Gamma_0(N)$, Amer. Math. Soc., Providence, 1989.
26. James E. Humphreys, *Linear algebraic groups*, Graduate Texts in Math., vol. 21, Springer-Verlag, New York, 1975.
27. K. lyanaga, *Arithmetic of special unitary groups and their symplectic representations*, J. Fac. Sci. Univ. Tokyo (Sec. 1) **15** (1968), no. 1, 35–69.
28. K. Iyanaga, *Class numbers of definite Hermitian forns*, J. Math. Soc. Jap. **21** (1969), 359–374.
29. Hervé Jacquet and Robert P. Langlands, *Automorphic forms on GL(2)*, Lectures Notes in Math., vol. 114, Springer-Verlag, Berlin, 1970.
30. C. Khare and J.-P. Wintenberger, *On Serre's conjecture for 2-dimensional mod p representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Ann. of Math. (2) **169** (2009), no. 1, 229–253.
31. Markus Kirschmer and John Voight, *Algorithmic enumeration of ideal classes for quaternion orders*, SIAM J. Comput. (SICOMP) **39** (2010), no. 5, 1714–1747.
32. Max-Albert Knus, *Quadratic and Hermitian forms over rings*, Springer-Verlag, Berlin, 1991.
33. Martin Kneser, *Klassenzahlen indefiniter quadratischer Formen in drei oder mehr Veränderlichen*, Arch. Math. **7** (1956), 323–332.
34. Martin Kneser, *Klassenzahlen definiter quadratischer Formen*, Arch. Math. **8** (1957), 241–250.
35. Martin Kneser, *Strong approximation*, Algebraic groups and discontinuous subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965), American Mathematical Society, Providence, 1966, 187196.
36. David Kohel, *Hecke module structure of quaternions*, Class field theory: its centenary and prospect (Tokyo, 1998), ed. K. Miyake, Adv. Stud. Pure Math., vol. 30, Math. Soc. Japan, Tokyo, 2001, 177–195.
37. Joshua Lansky and David Pollack, *Hecke algebras and automorphic forms*, Compositio Math. **130** (2002), no. 1, 21–48.

38. M.A.A. van Leeuwen, A.M. Cohen, and B. Lisser, *LiE, a package for Lie group computations*, CAN, Amsterdam, 1992.
39. David Loeffler, *Explicit calculations of automorphic forms for definite unitary groups*, LMS J. Comput. Math. **11** (2008), 326–342.
40. Markus Kirschmer and John Voight, *Algorithmic enumeration of ideal classes for quaternion orders*, SIAM J. Comput. (SICOMP) **39** (2010), no. 5, 1714–1747.
41. O. Timothy O'Meara, *Introduction to quadratic forms*, Springer-Verlag, Berlin, 2000.
42. Arnold Pizer, *An algorithm for computing modular forms on* $\Gamma_0(N)$, J. Algebra **64** (1980), vol. 2, 340–390.
43. Wilhelm Plesken and Bernd Souvignier, *Computing isometries of lattices*, Computational algebra and number theory (London, 1993), J. Symbolic Comput. **24** (1997), no. 3–4, 327–334.
44. Winfried Scharlau, *Quadratic and Hermitian forms*, Springer-Verlag, Berlin, 1985.
45. Alexander Schiemann, *Classification of Hermitian forms with the neighbour method*, J. Symbolic Comput. **26** (1998), no. 4, 487-508.
46. Rudolf Scharlau and Boris Hemkemeier, *Classification of integral lattices with large class number*, Math. Comp. **67** (1998), no. 222, 737–749.
47. Rainer Schulze-Pillot, *An algorithm for computing genera of ternary and quaternary quadratic forms*, Proc. Int. Symp. on Symbolic and Algebraic Computation, Bonn, 1991.
48. Goro Shimura, *Arithmetic of unitary groups*, Ann. of Math. (2) **79** (1964), 369–409.
49. Jude Socrates and David Whitehouse, *Unramified Hilbert modular forms, with examples relating to elliptic curves*, Pacific J. Math. **219** (2005), no. 2, 333–364.
50. William Stein, *SAGE Mathematics Software* (version 3.1.1), The SAGE Group, 2008, `http://www.sagemath.org/`.
51. John Voight, *Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms*, accepted, `arXiv:1004.0994`.
52. Hermann Weyl, *The classical groups: their invariants and representations*, Princeton University, Princeton, 1966.